REMARKS

In the Office Action, the Examiner rejected claims 42, 69, and 77 under 35 U.S.C. § 112, ¶ 2, as allegedly being indefinite.[1] In addition, the Examiner rejected claims 42-82 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,804,355 (*Graunke*) in view of U.S. Patent No. 5,261,003 (*Matsui*). In this response, Applicant amends independent claims 42, 69, and 77. Support for these amendments can be found in the originally-filed specification at, for example, page 6, line 29 to page 7, line 9, and Figs. 5 and 6. No new matter has been added. Applicant has also amended dependent claims 46-48, 50-52, 57, and 63-67 for clarity. Accordingly, claims 42-82 are currently pending, of which claims 42, 69, and 77 are independent. Applicant respectfully traverses all pending rejections for at least the following reasons.

Rejection Under 35 U.S.C. § 112, ¶ 2

Claims 42, 69, and 77 stand rejected under 35 U.S.C. § 112, ¶ 2, for allegedly being indefinite. More particularly, the Office Action alleges that the recitations of the variable "k," "N," and "n+m" in the independent claims render the scope of these claims indefinite. *See* Office Action, p. 2.

Without conceding to the Office Action's allegation, Applicant has amended independent claims 42, 69, and 77 in order to improve clarity. For example, Applicant has changed "input digital data of word size N" to "input digital data having a first word size" in claims 42 and 77. Similar changes have been made to clarify the scope of the

---

[1]   The Office Action contains a number of statements characterizing the Applicant's disclosure, including the claims, and the related art. Regardless of whether any such statement is specifically addressed herein, Applicant declines to automatically subscribe to any statement or characterization in the Office Action.

previously recited variables "k" and "m+n" in independent claims 42, 69, and 77.

Applicant has also amended dependent claims 47, 48, 50, 51, and 63-67 to remove any

recitations of variables such as the variable "k." Applicant therefore submits that claims

42, 69, and 77 fully comply with the provisions of 35 U.S.C. § 112, second paragraph

and respectfully request withdrawal of the rejection.

Rejections Under 35 U.S.C. § 103(a)

Applicant respectfully traverses the rejection of claims 42-82 under 35 U.S.C.

§ 103(a) as being unpatentable over *Graunke* in view of *Matsui*. The Office Action has

not properly resolved the *Graham* factual inquiries, the proper resolution of which is the

requirement for establishing a framework for an objective obviousness analysis. *See*

M.P.E.P. § 2141(II), citing to *Graham v. John Deere Co.*, 383 U.S. 1, 148 U.S.P.Q. 459

(1966), as reiterated by the U.S. Supreme Court in *KSR Int'l Co. v. Teleflex Inc.*, 550

U.S. 398, 82 U.S.P.Q.2d 1385 (2007).

While Applicant has amended independent claims 42, 69, and 77 to further

demonstrate the differences between *Graunke* and the claims, Applicant maintains that

the Office Action has not properly ascertained the differences between the claims and

the references, at least because it has not interpreted the references and considered

both the claims *and* the prior art *as a whole*. *See* M.P.E.P. § 2141(II)(B). Accordingly,

the Office Action has not clearly articulated a reason why the claimed invention would

have been obvious, which is "[t]he key to supporting any rejection under 35 U.S.C. 103."

M.P.E.P. § 2143.

Representative claim 42, as amended, calls for a combination including, for

example,

a multiplexer circuit that receives a first portion of said input block of bits and a first set of key bits as inputs, the first portion of said input block of bits operable to select a second set of key bits out of the first set of key bits, wherein the selected second set of key bits are output by said multiplexer circuit

Applicant respectfully submits that neither *Graunke* nor *Matsui*, either alone or in combination, teaches or suggests at least this element of Applicant's amended independent claim 42.

Graunke generally discloses a "block cipher includ[ing] a recursive Feistal network structure having a plurality of substitution boxes (S-boxes), each S-box being generated by a message digest function used as a pseudo-random number generator and one of a plurality of keys." *Graunke*, col. 1, ll. 43-48. In one embodiment of the disclosed block cipher, "[p]laintext data input to the block cipher may be represented by registers denoted plaintext high (PH) 100 and plaintext low (PL) 102." *Id.* at col. 3, ll. 54-56. Then,

[t]he data from PH 100 may be input into a pseudo random function R (FR) 104. . . . Within FR 104, the PH data may be split into two halves, register A 108 and register B 110. . . . The data from register B may be input into a pseudo random function S (FS) 112. FS may be a substitution array (S-box). FS partially encrypts B's data . . . .

Id. at col. 4, ll. 1-11. *Graunke* further discloses that within the S-box, "a permutation of integers . . . may be computed using the message digest as a . . . pseudo-random number generator (RNG) and the key. The generated integers may be used within the S-box as part of a look up table for shuffling the input data . . . into encrypted output data." *Id.* at col. 2, ll. 58-63.

The Office Action appears to equate the "pseudo random function S-Box, FS" disclosed by *Graunke* to the claimed "multiplexer circuit." *See* Office Action, pp. 3-4.

This reasoning is incorrect for at least two reasons. First, as shown above, instead of disclosing that S-Box FS "receives a first portion of said input block of bits and a first set of key bits as inputs," as required by amended claim 42, *Graunke* discloses that "[t]he data from register B [is] input into a pseudo random function S (FS) 112." *Graunke*, col. 4, ll. 8-9. *Graunke* appears to contain no disclosure that S-box FS receives a first set of key bits as a second input. *See, e.g., id.* at Fig. 1 (showing that S-box FS receives a single input, the data from register B).

Second, *Graunke's* S-box cannot constitute the claimed "multiplexer circuit" because *Graunke* does not disclose that "the first portion of said input block of bits [is] operable to select a second set of key bits out of the first set of key bits, wherein the selected second set of key bits are output by said multiplexer circuit," as recited by amended independent claim 42. Instead of disclosing that data from register B, which is input into S-box FS, *selects key bits* that are then output by the S-box, *Graunke* discloses that "FS partially encrypts B's data." *Graunke*, col. 4, l. 10. Indeed *Graunke* discloses elsewhere that "a permutation of integers [is] computed" in the S-box "using the message digest [function] as a . . . pseudo-random number generator (RNG) and the key. The generated integers may be used within the S-box as part of a look up table for shuffling the input data . . . into encrypted output data." *Id.* at col. 2, ll. 58-63. In other words, *Graunke* appears to disclose that some of the data from register B is replaced with integers that have been randomly generated in the S-box to allow the S-box to output partially encrypted data.

Accordingly, the S-box FS of *Graunke* does not correspond to the "multiplexer circuit that receives a first portion of said input block of bits and a first set of key bits as

inputs, the first portion of said input block of bits operable to select a second set of key

bits out of the first set of key bits, wherein the selected second set of key bits are output

by said multiplexer circuit," as recited in amended independent claim 42.

      Matsui does not cure the above-noted deficiency of *Graunke*. *Matsui* generally

discloses "a data communication system and method with a data scrambling." *Matsui*,

col. 1, ll. 7-8. To that end, *Matsui* discloses that in its system,

> the input plaintext 3 is divided into more significant 4 bytes and less
> significant 4 bytes, and the less significant 4 bytes are input to the
> processing block 9 and the address calculating circuit 23 through the
> selector 24. The address calculating circuit 23 calculates and [sic]
> address of a [sic] extended key to be selected on the basis of the input
> plaintext data and outputs the calculated address to the extended key
> latch 7. The extended key latch 7 supplies the selected extended key
> corresponding to the given address to the selector 25, and the key is
> transmitted to the processing block 9 through the selector 25. The
> processing block 9 scrambles the input plaintext data by using the
> selected key of the selector 25 as the parameter and outputs a scrambled
> data.

Id. at col. 6, ll. 4-18.

      Although *Matsui* discloses two selectors, it does not disclose "a multiplexer circuit

that receives a first portion of said input block of bits and a first set of key bits as inputs,"

as recited by amended independent claim 42. Instead, as shown above, *Matsui*

discloses one selector that receives the 4 less significant bits of input plaintext as an

input (selector 24) and another selector that receives an extended key as an input

(selector 25). *See id.* In other words, neither selector 24 nor selector 23 can constitute

the claimed "multiplexer circuit" because neither receive both the 4 less significant bits

of the input plain text and the extended key as an input. Accordingly, *Matsui* fails to

cure the above-referenced deficiency of *Graunke*.

As set forth above, *Graunke* and *Matsui* do not teach or suggest every feature of Applicant's amended independent claim 42. Consequently, the Office Action has not properly ascertained the differences between the references and the rejected claim. Accordingly, no reason has been clearly articulated as to why the claim would have been obvious to one of ordinary skill in the art. For at least this reason, claim 42 should be allowable.

Applicant's amended independent claims 69 and 77, although different in scope from amended independent claim 42, recite similar subject matter and are therefore allowable for at least the same reasons. Dependent claims 43-68, 70-76, and 78-82, each depend from one of independent claims 42, 69, and 77, and are therefore allowable for at least the same reasons. Applicant therefore respectfully requests that the rejection of claims 42-82 under 35 U.S.C. § 103(a) be withdrawn.

Conclusion

In view of the foregoing amendments and remarks, Applicant respectfully requests reconsideration and reexamination of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to Deposit Account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: March 9, 2010   By:_____

R. Bruce Bower
Reg. No. 37,099